Illinois Office of Health Information Technology

ILHIE Update

July 17, 2012

Laura Zaremba

OHIT Director and ILHIE Acting Executive Director

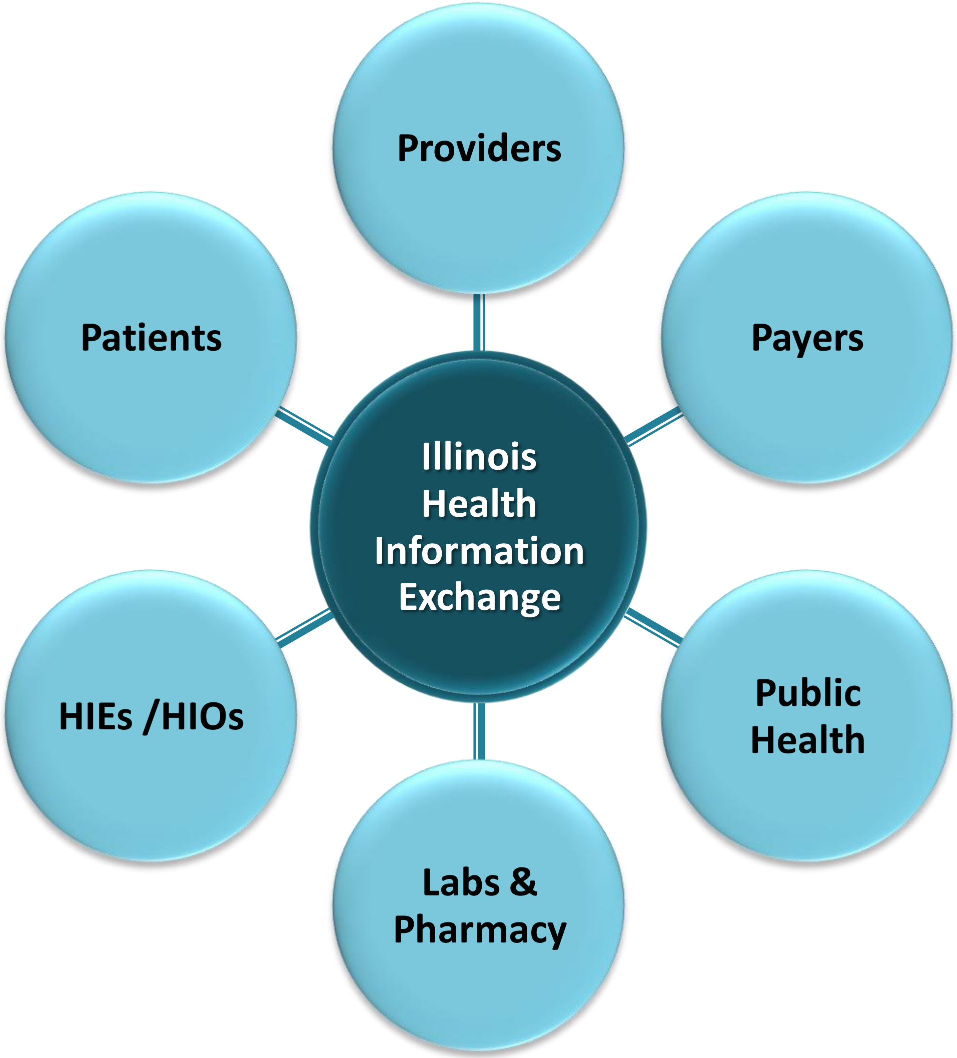
Agenda

- Overview of the architecture and implementation status of the ILHIE

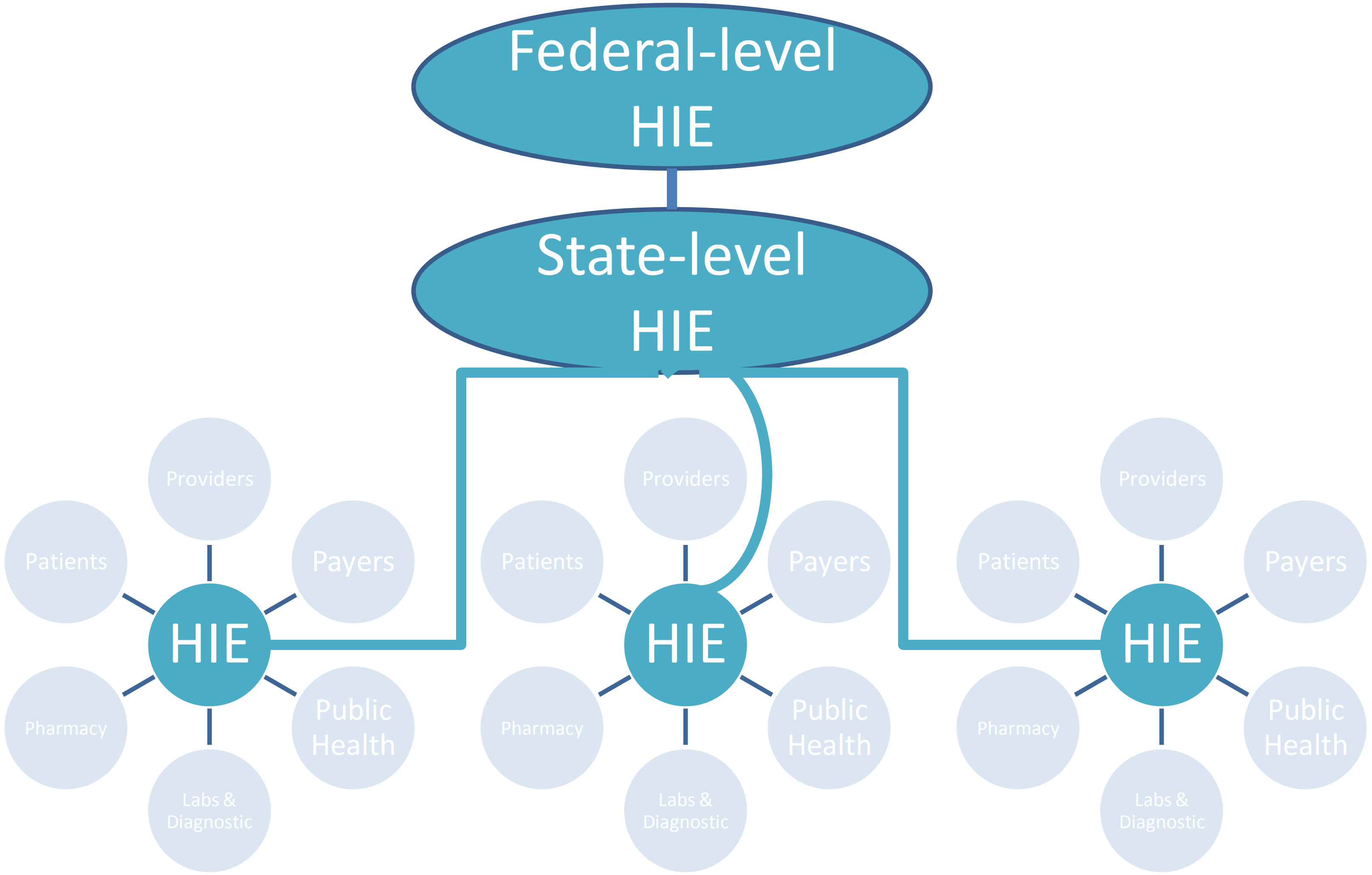
- Overview of the patient data privacy & security implications of HIE networks

HIE network hub concept

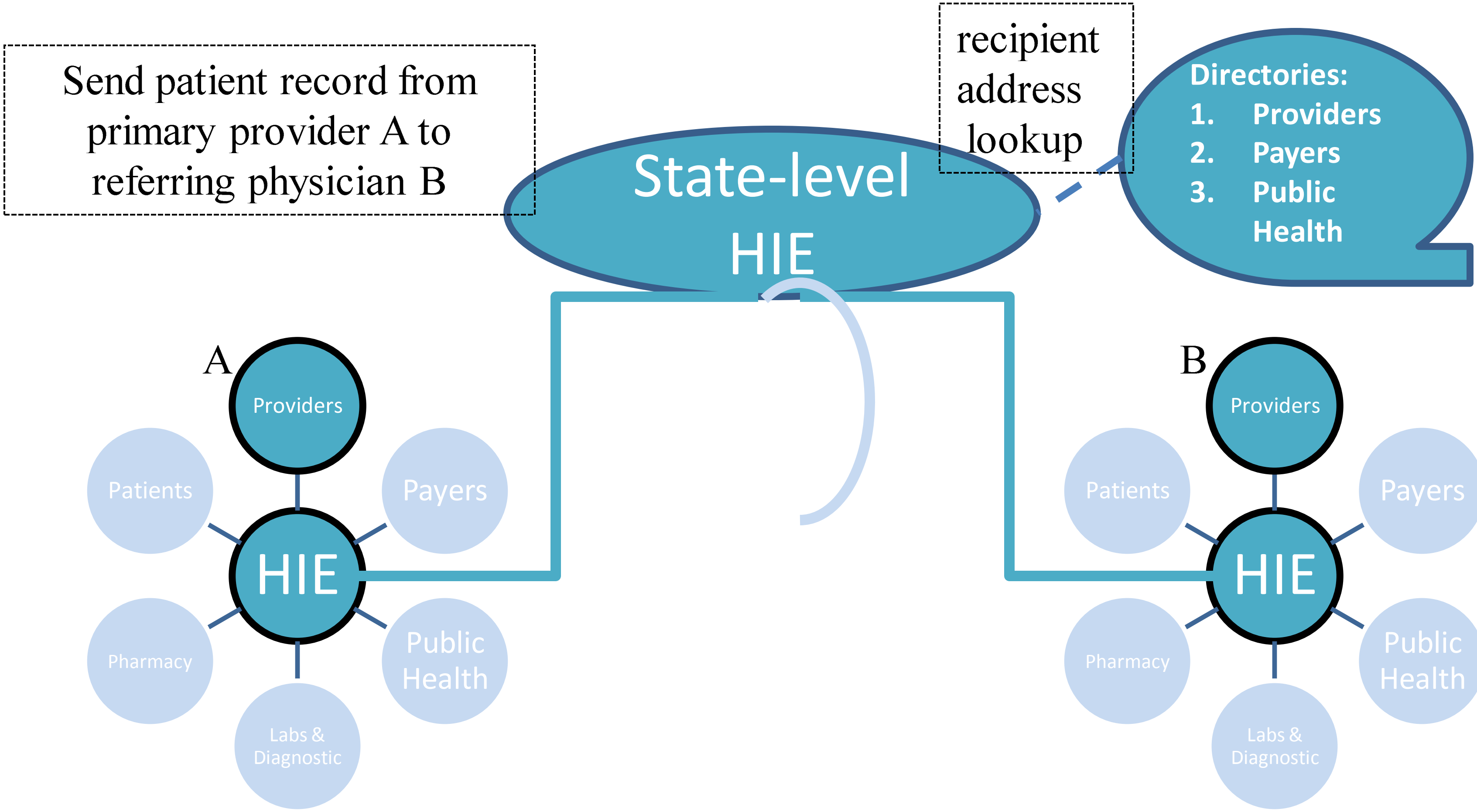
Secure, effective, and efficient exchange of health information in compliance with state and federal standards, laws, and regulations



HIE concept: federated networks



HIE service: Directed Message (Uni-directional) Exchange ("push")

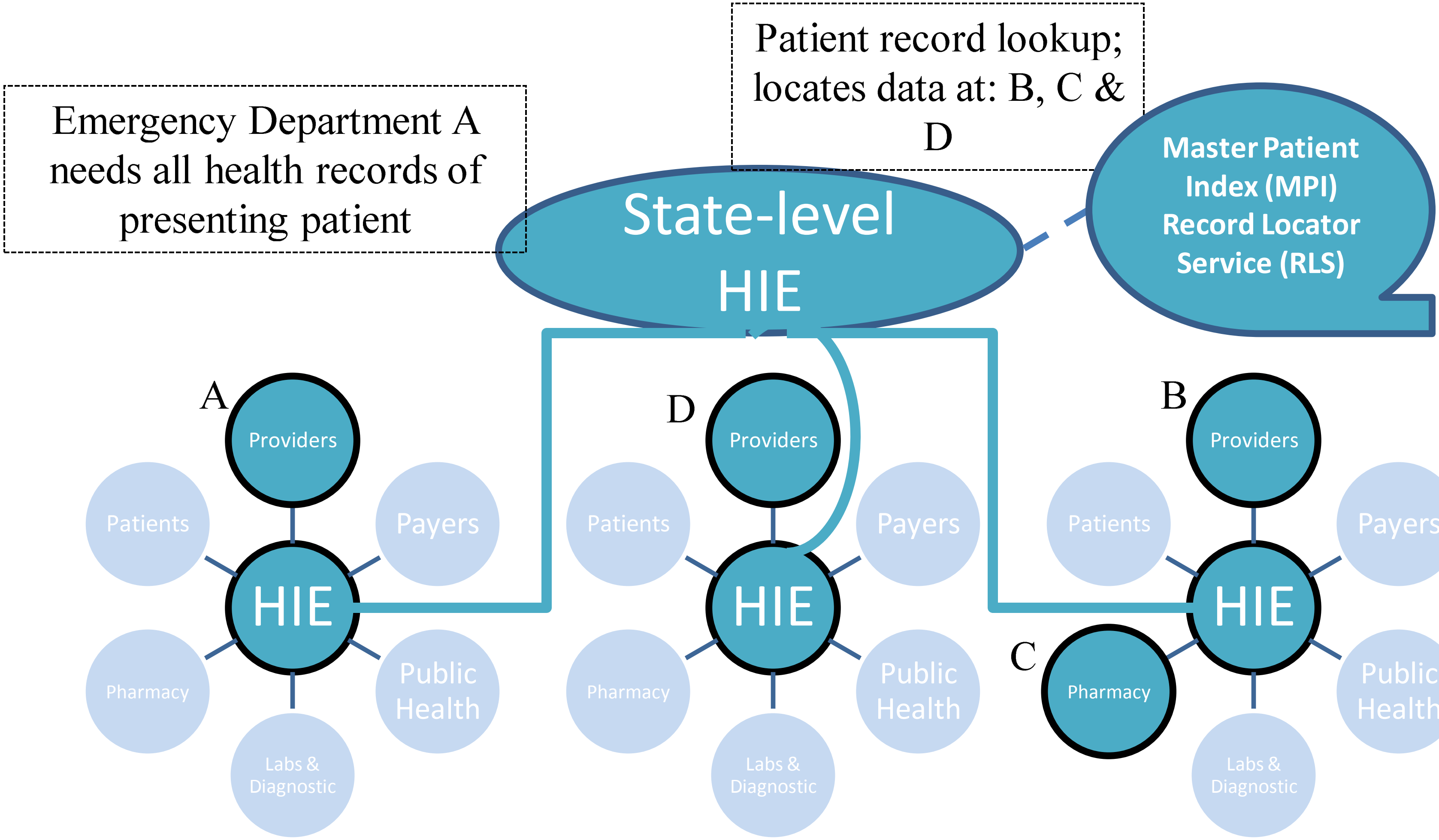


Send patient record from primary provider A to referring physician B

recipient address lookup

Directories:
1. Providers
2. Payers
3. Public Health

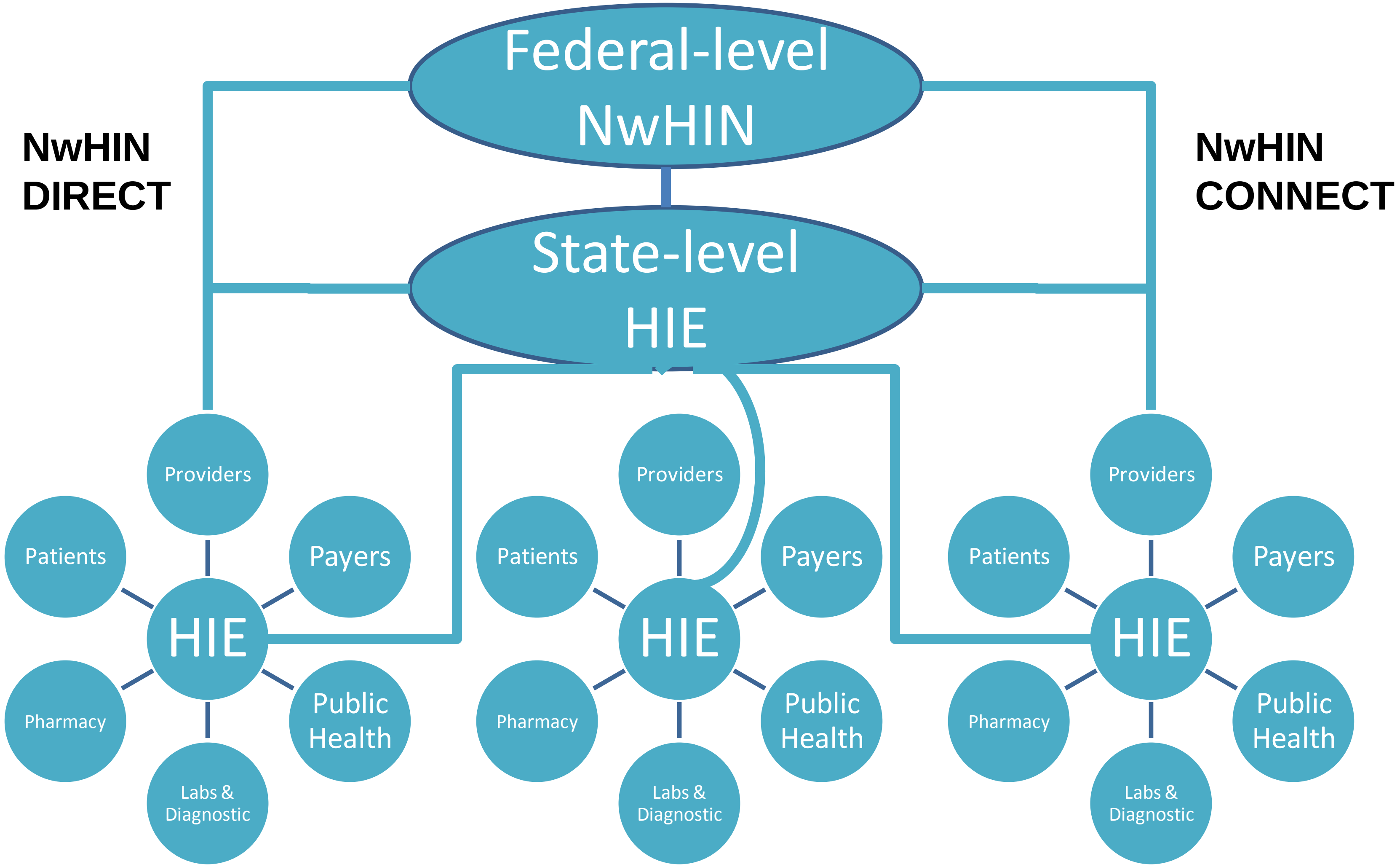
HIE service: Aggregated Data (Bi-directional) Query-Response ("pull")



Emergency Department A needs all health records of presenting patient

Patient record lookup; locates data at: B, C & D

HIE network concept has evolved

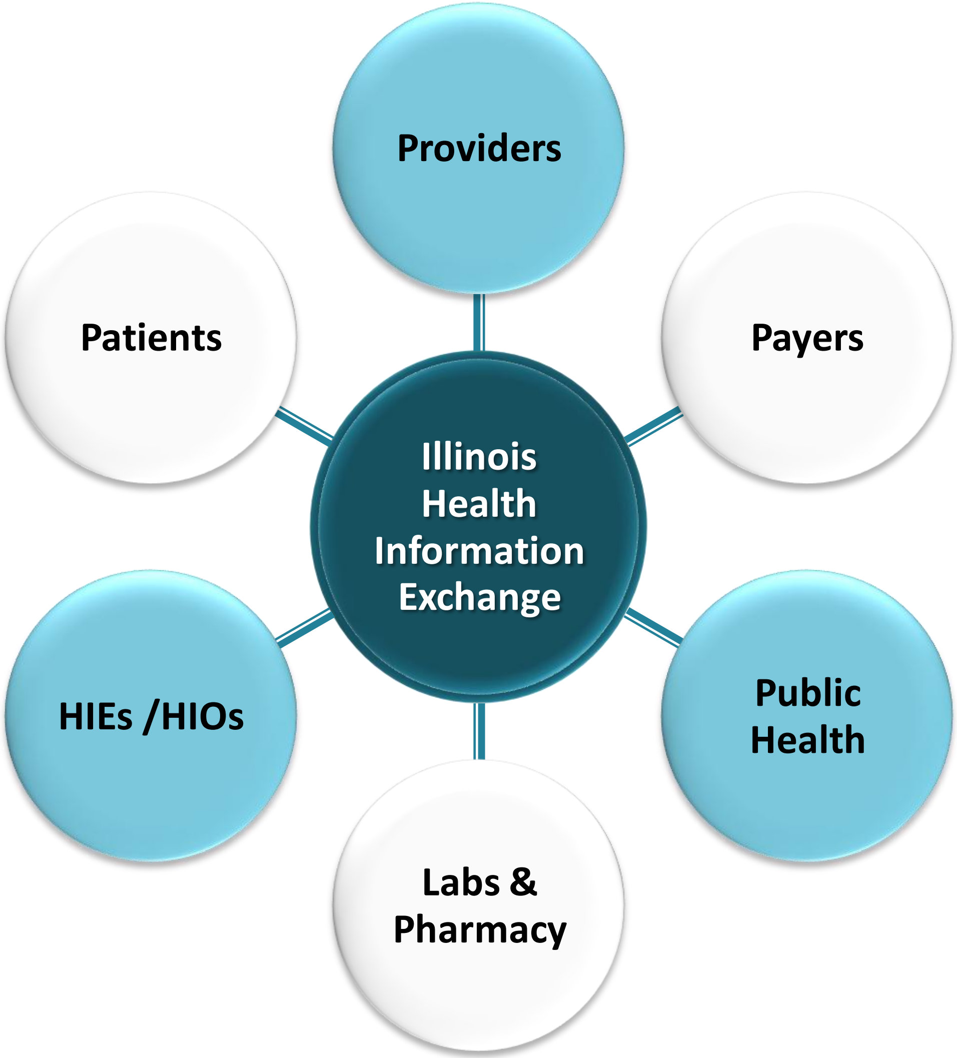


ILHIE Development Strategy

Phase 1: Direct Messaging (uni-directional; push)

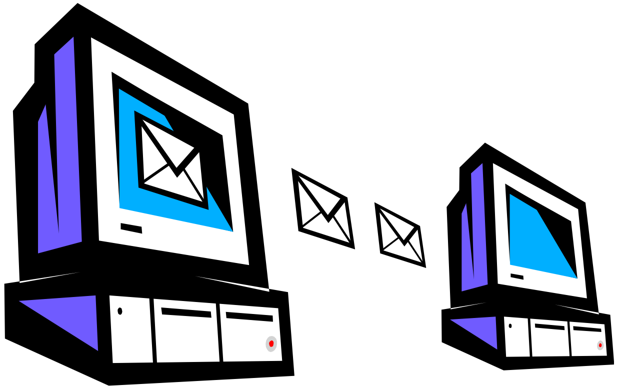
Phase 2: Aggregated Data (bi-directional; query-response; pull)

Focus:
Meaningful Use
Transitions of care
Care coordination



ILHIE Phase I: Direct Messaging

- ILHIE launched Direct secure messaging service Dec. 2011
  - Similar to using e-mail
  - Encrypted message transport to other enrolled Direct users
  - Enrollment requires user identity verification
  - No cost to Illinois providers through 2012



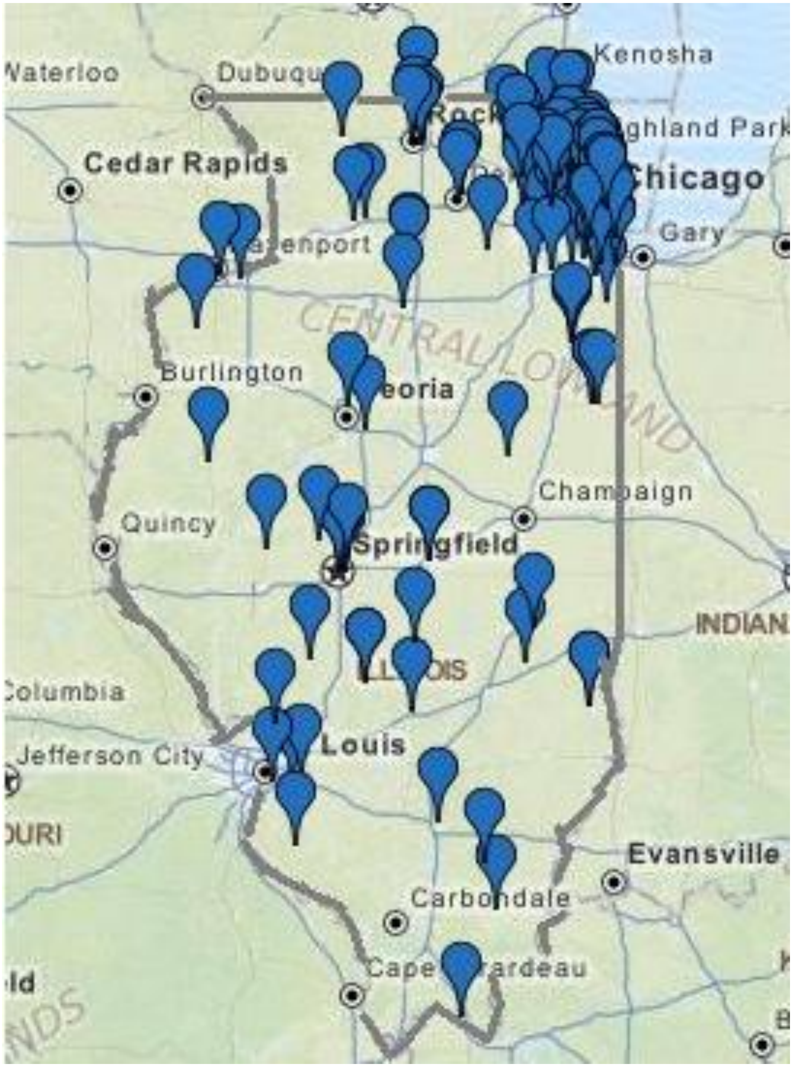
Direct Messaging – Use Cases

Designed to address multiple use cases

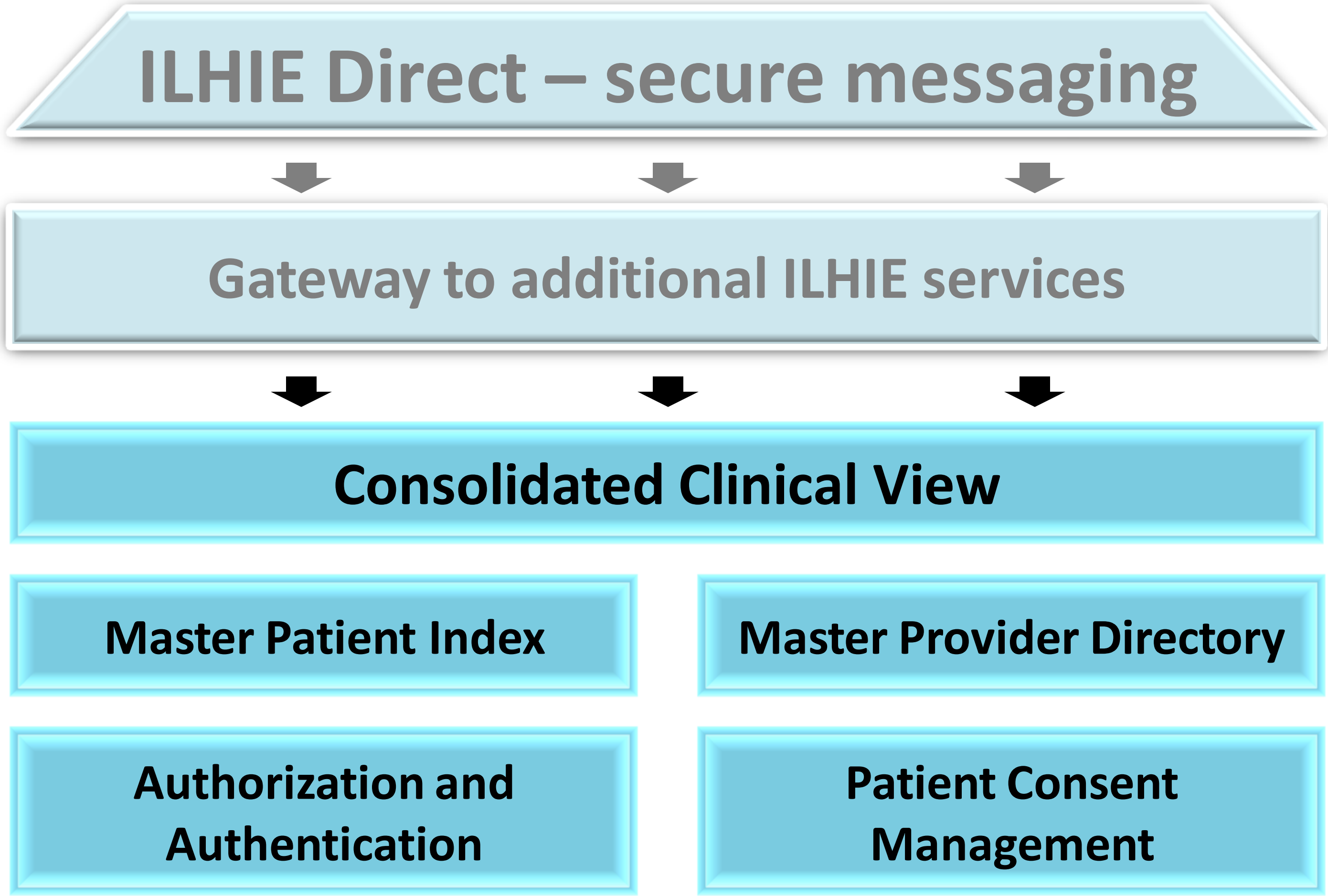
- **Behavioral Health Care Integration** – protected information is sent securely under existing consent laws and policies
- **Emergency Department Alerts** – send alerts to physicians when their at-risk patients are admitted through the ED
- **Specialist Referral Coordination** – transmit relevant and timely info about the patient
- **Transitions of Care** – send patient care summaries during care transitions

ILHIE Direct Participants

📍 Denotes each ILHIE Direct address account location, not individual contacts.



Gateway to more robust HIE



ILHIE Direct – secure messaging

Gateway to additional ILHIE services

Consolidated Clinical View

Master Patient Index

Master Provider Directory

Authorization and Authentication

Patient Consent Management

ILHIE Phase 2: Aggregated query-response (bidirectional exchange)

- In 2011 ILHIE retained a technology vendor, InterSystems Corporation, to provide a robust "Software-As-A-Service" HIE solution

- Core components:
  - Master Patient Index/Record Locator Service
  - Data aggregation engine
  - Secure data transport/display
  - Directories: Providers, Public Health Authorities

- Use cases:
  - 1. Emergency room "pull" of aggregated PHI
  - 2. Clinical specialist referrals (using Provider Directory)
  - 3. Public health reporting via special node
  - 4. Provider incentive payment reporting

Phase 2 implementation status

- In test phase for bidirectional exchange
  - Testing Master Patient Index,
  - Populating Master Provider Directory
  - Will begin testing Public Health Node connectivity (late 2012)

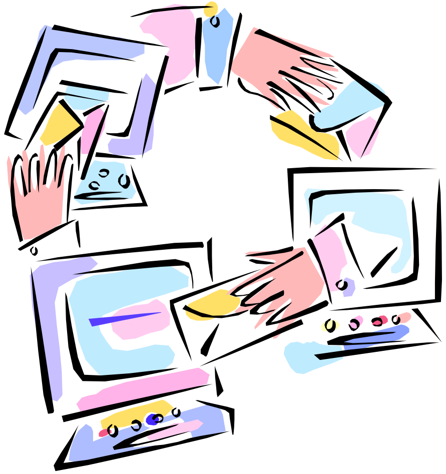
- Current on-boarding pipeline
  - Chicago and southern Illinois-based FQHCs
  - Hospitals in multiple regions
  - Regional HIE in central Illinois

- Estimate 2 to 6 month test period

- Privacy & Security/Patient Consent Management implications for HIE

Sharing of Clinical Data Is Key

- Health care ecosphere is complex
- Successful treatment of a single patient involves multiple parties
  - Clinical treatment is delegated among multiple specialists
  - Location of clinical treatment is distributed among different types of facilities during patient's course of treatment
  - Payment for treatment from multiple sources
  - Management of multiple parties and processes requires evaluation systems which measure and assess results



Accommodation of multiple interests

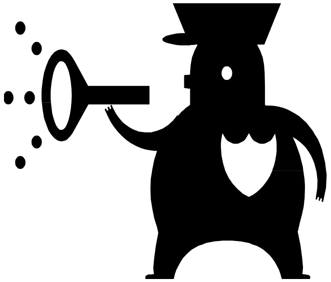
- Multiple parties contribute to the creation of patient data and **multiple parties have interests** in the use and sharing of such patient data, including: patients; providers; payers; public health authorities

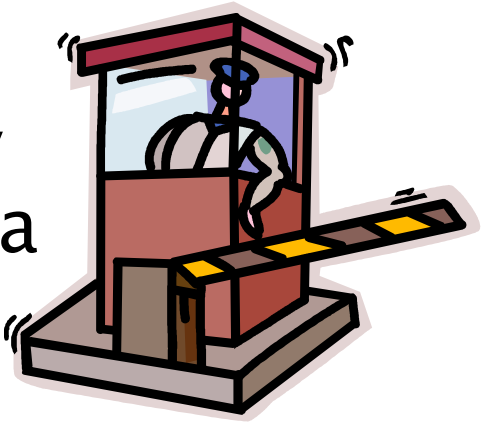
- Accommodation of these multiple interest is an **issue of policy and politics**, less an issue of technology
  - Importance of diverse stakeholder input to ILHIE Authority
  - Focal point of health care policy: the patient

- **Patients have concerns** regarding potential uses of health care data, e.g. adverse insurance coverage determinations or employment decisions

PHI "Misuse" Laws & "Gatekeeper" Laws

- Addressing patient concerns regarding potential "misuse" of patient health data – 2 methods of legal protection:
  - **"misuse" laws** – restricting use of PHI, e.g. by insurance companies and employers
  - **"gatekeeper" laws** – restricting initial release of data, principally by requiring patient consent for a release





Old Laws >< New Technologies

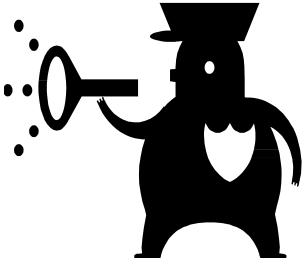
- Most patient PHI privacy laws fashioned prior to the digital (EHR/HIE) revolution
  - Applied generally to point-to-point (unilateral directed exchange), usually involving a single point of release, a single data custodian, and a single recipient
- Today's challenge: how to take advantage of new HIT technologies while accommodating stakeholder interests affected by the new technologies?
  - Today's aggregated PHI query-response (bilateral exchange) HIEs involve multiple points of release, multiple data custodians, multiple recipients – not all known to all parties at the time of the data release

HIE operational criteria: completeness & prompt delivery

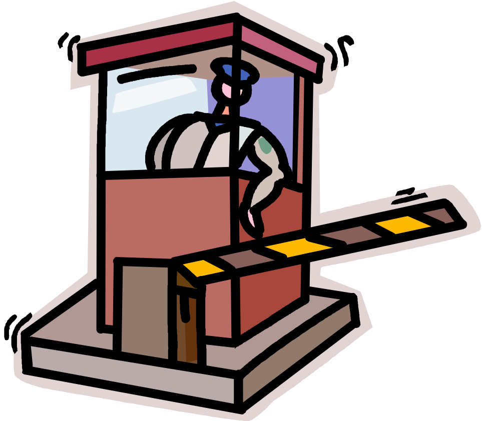
For HIE to facilitate patient treatment:

- providers desire access to complete patient record
- data needs to be delivered on demand

With regard to HIE data flows:



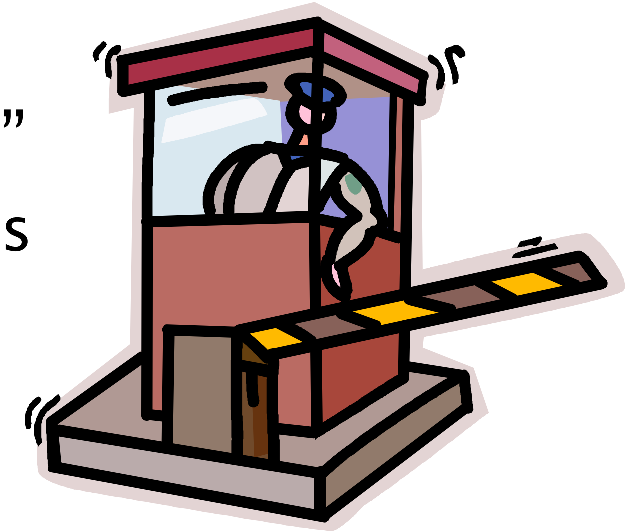
- "misuse" laws – generally involve data use audits after data is released for use



- "gatekeeper" laws – generally require action by custodian of data; potentially impacts both "completeness" and "prompt delivery" of data for use

Specially-protected PHI

- “Gatekeeper” laws generally protect patient health data considered “highly confidential”
  - Mental health; psychotherapy notes
  - Substance abuse
  - HIV/AIDS
  - Genetic Testing



IL mental health confidentiality law (MHDDCA)

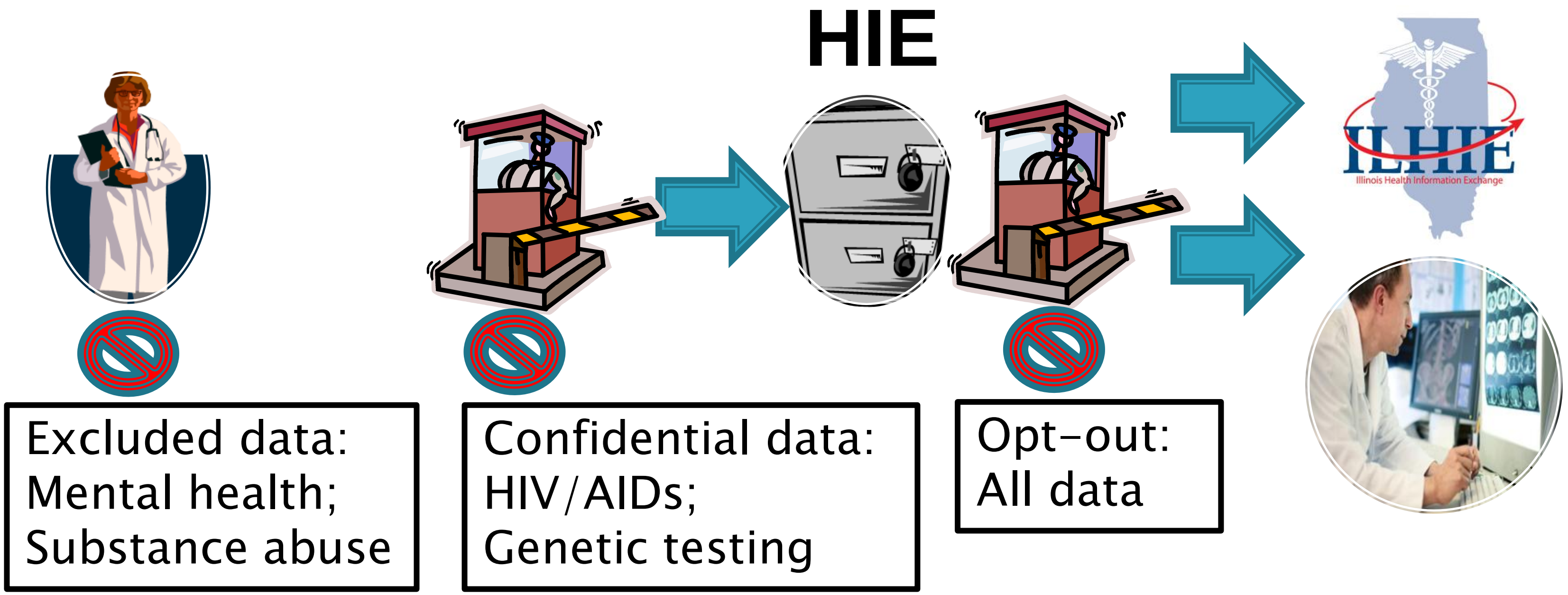
- MHDDCA requires patient consent with considerable specificity for release of data
  - Prohibits “blanket consent”
  - Prohibits “advance consent”
  - Durational limit on consent

- MHDDCA application unclear and arguably restricts data aggregation query-response HIE to disclose data without a new consent at the time of each data release
  - Future data recipients not known (at data creation)
  - Date of future data release not known

MetroChicago-HIE data filters

MetroChicago-HIE data filters

- “Excluded data”: mental health; substance abuse
- “Highly Confidential data”: HIV/AIDS; genetic testing



Excluded data:
Mental health;
Substance abuse

Confidential data:
HIV/AIDs;
Genetic testing

Opt-out:
All data

MetroChicago-HIE data filters

- Consequences:
  - All free text data is suppressed, for all patients
  - All patients with any mental health data trigger are excluded
- Filtering of data by RHIO intermediaries has potentially adverse effect upon ILHIE access to patient data